## ABSTRACT OF THE INVENTION

In computer environments where passwords are used to compute retained secrets by methods such as password-based encryption, a need often arises to update these secrets. Retaining the password value, or the keys computed from the password, would be unwise; and requiring each password owner to type in their password would be cumbersome. The present invention describes a method that allows a fully operational system to modify the retained secrets without retaining passwords or requiring human intervention.